IN THE CLAIMS

Please amend claims 1 and 3-6.

The pending claims are therefore as follows:

1. (currently amended): A method of production and distribution of asymmetric public and private keys to provide certifications of transactions, comprising the steps of:

- providing a key generation center in charge of generating a plurality of asymmetric public and private keys to be used to provide certificates of transactions,
- generating certificates comprising a public key and a private key in a first cryptographic unit (KPG) of the key generation center,
- coding the private key by means of a secret service key in the key generation center in the first cryptographic unit (KPG) and storing said coded private key in a key memory (KPS) of the key generation center,
- when ~~sending~~ preparing to send the public and private keys to a user unit, extracting the keys from the key memory (KPS), and composing the certificates with the public key,
- decoding the corresponding private key by means of a service key in a cryptographic security module and coding it with a transport key of the user~~.~~,
- sending the public key and the encrypted private key to a user unit.

2. (original): A method according to Claim 1, characterised in that the encrypted private key is received by the user unit (DEC) and transmitted to the security module (SM) containing the transport key for decoding and storing the private key.

3. (currently amended): A method according to Claim 1, characterised in that it ~~consists in~~ comprises using several monolithic cryptographic unit to obtain a high speed coding module.

4. (currently amended): A method according to claim 1, characterised in that it ~~consists in~~ comprises:

- coding the public key of the centre with the transport key and transmitting it to the user unit (DEC),
- receiving by the user unit, the encrypted public key and transmitting it to the security module (SM),
- decoding and storing the public key by means of the transport key inside the security module (SM).

5. (currently amended): A method according to claim 2, characterised in that it ~~consists in~~ comprises:

- coding the public key of the centre with the transport key and transmitting it to the user unit (DEC),
- receiving by the user unit, the encrypted public key and transmitting it to the security module (SM),
- decoding and storing the public key by means of the transport key inside the security module (SM).

6. (currently amended): A method according to claim 3, characterised in that it ~~consists in~~ comprises:

- coding the public key of the centre with the transport key and transmitting it to the user unit (DEC),
- receiving by the user unit, the encrypted public key and transmitting it to the security module (SM),
- decoding and storing the public key by means of the transport key inside the security module (SM).